ABSTRACT

Security is a vital requisite for communication systems. Speech scramblers are gaining wide spread acceptance as a mean of enhancing protection in both military and civilian application.

Increasing interest in speech scramblers is attributed to the desire for secure speech cmmunications over existing telephone channels with standard telephone bandwidth at acceptable speech quality and reasonable cost.

This work presents simulation methods for different kinds of scrambling systems (one or two dimensional) and compare between them. The main work is in applying a complete scrambling system on a single FPGA using Foundation 2.1i.

Different types of scrambling systems in different domains are simulated using Borland C++ object language. These systems are tested to decide which type to implement.

The keys used through the tests were generated using MATLAB, and the key used in implementation of FPGA used Schematic Editor of Foundation 2.1i. The generation of permutation keys is selected according to several parameters, to specify level of security for each key. These parameters is performed using the Weighted Mobile Average (WMA) and the Weighted Shift Parameters (WSP) for frequency keys and the Temporal distance (d) for time keys.

Tests are made using four types of objective tests, that include Spectral Segmental Signal to Noise Ratio (SSNRseg), Segmental Signal to Noise Ratio (SNRseg), Log Likelihood Ratio (LLR) measures, and Cepstral Distance (CD) measure.

Computer simulation results strongly support the theories. It shows that two dimensional (frequency scrambling after FFT with filter bank using Hamming window ended by time scrambling) gives high secure scrambling system with pure recovered speech.

The design and implementation of scrambling system include the design and implementation of Radix – 2 FFT butterfly, permutation and IFFT using single FPGA specify that approximatly real time speech scrambling system becoming available using FPGA

PDF created with pdfFactory trial version www.pdffactory.com

الخلاصة

أصبحت الأمنيّة الأكثر ضرورية وأساسية لأنظمة الأتصالات على الأطلاق، لذا فأن المُبعثرات الصوتية أكتسبت قبولاً واسع الأنتشار كوسيلة لحماية كل من الأتصالات المدنية والعسكرية.

توجد رغبة متزايدة في المبعثرات الصوتية بسبب الرغبة في أتصال صوتي مُؤمّن عبر خطوط الهاتف الموجودة ،على حزمة ترددية هاتفية قياسية ،ونوعية صوت مقبولة وكلفة معقولة.

يقدم هذا العمل طرق مختلفة لمحاكاة أنواع مختلفة من أنظمة البعثرة (ذات البعد الواحد أو البعدين) والمقارنة بينهم لذا فإن العمل الرئيسي هو تنفيذ نظام بعثرة كامل بأستخدام(FPGA) بمساعدة النظام الأساس (2.1 i)٠

هنالك أنواع مختلفة لمبعثرات صوتية في حقول مختلفة حوكيت برمجياً بأستخدام لغة Borland C++ ذات الشئ الموجه٠ هذه الأنظمة أختبرت لتقرير أي نوع سوف ينفذ.المفاتيح التي أستخدمت خلال الأختبار ولّدت بأستخدام برنامج MATLAB ، والمفتاح المستخدم بتنفيذ الـ(FPGA) والذي يعمل بطريقة المحرّر التخطيطي للبرنامج الأساس(2.1 i)٠أن توليد مفاتيح التباديل تم أختيارها بالأعتماد على بضعة عوامل ، لتحديد مستوى الأمنيّة لكل مفتاح ، هذه العوامل هي معدل التحرك الموزون(WMA) وعامل الأزاحة الموزون (WSP) لمفاتيح التردد ، والمسافة الزمنية(d) لمفاتيح الزمن٠الأختبار تم بأستخدام أربعة أنواع من الأختبارات الموضوعية ، وهي نسبة الأشارة الى الضوضاء المقطعية الطيفية($SSNR_{seg}$) ، ونسبة الأشارة الى الضوضاء المقطعي (SNR_{seg})، ومقياس النسبة اللوغاريتمية الترجيحية(LLR)، ومقياس المسافة السبسترالي(CD)٠

ان نتائج المحاكاة الحاسوبية تدعم وبقوة النظريات ، ومحرّر التخطيط المستخدم مع البرنامج الأساس (2.1 i) والذي تم بموجبه تنفيذ النظام ككل بأستخدام قطعة واحدة من (FPGA)، حيث أنه بيّن أن نظام البعثرة الصوتية أستغرق زمن مقارب الى الزمن الحقيقي وبأستخدام مكونات صلبة قليلة من CLB المطلوبة للـ (FPGA)٠

PDF created with pdfFactory trial version www.pdffactory.com